

Bypass Rewiring and Robustness of Complex Networks

Junsang Park^{1,*} and Sang Geun Hahn^{1,2}

¹*Graduate School of Information Security,*

Korea Advanced Institute of Science and Technology,

291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

²*Department of Mathematical Sciences,*

Korea Advanced Institute of Science and Technology,

291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

(Dated: July 1, 2016)

Abstract

A concept of bypass rewiring is introduced and random bypass rewiring is analytically and numerically investigated with simulations. Our results show that bypass rewiring makes networks robust against removal of nodes including random failures and attacks. Especially, random bypass rewiring connects all nodes except the removed nodes on an even degree infinite network and makes the percolation threshold 0 for arbitrary occupation probabilities. In our example, the even degree network is more robust than the original network with random bypass rewiring while the original network is more robust than the even degree networks without random bypass. We propose a greedy bypass rewiring algorithm which guarantees the maximum size of the largest component at each step, assuming which node will be removed next is unknown. The simulation result shows that the greedy bypass rewiring algorithm improves the robustness of the autonomous system of the Internet under attacks more than random bypass rewiring.

PACS numbers: 89.75.Hc, 64.60.ah, 05.10.-a

* juns85@kaist.ac.kr

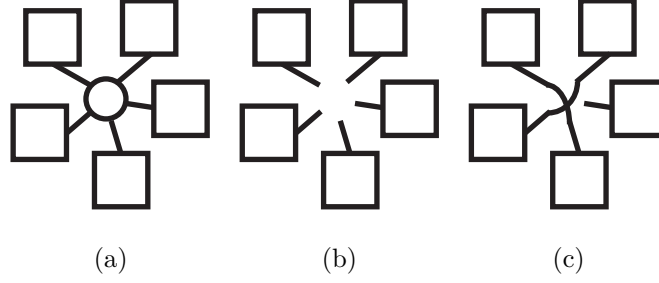


FIG. 1. A circle is for a node and squares are for components. (a) Before removal of the node, one node and five components are connected. (b) After removal of the node, the network fragments into five smaller components without bypass rewiring. (c) After removal of the node, the network fragments into two larger components and one smaller component with bypass rewiring.

Many real world systems (the Internet, electric power grids, the World Wide Web, social networks, urban streets, airline routes, subway, and so on) are represented by complex networks with many nodes and many links between nodes [1–13]. Networks (graphs) break into small disconnected parts when nodes are deleted. Complex networks are robust against random failures or error (random removal of nodes) but fragile and vulnerable to (intentional) attacks (targeted removal of nodes in decreasing order of degree from the highest degree) [1–3, 5, 7–10, 13–16]. There are various mitigation methods which make networks more robust [12, 17–19]. However, there are geographical, economic, and technical problems to implement the mitigation methods known so far. Therefore, we propose a concept of bypass rewiring to make networks robust against random failures and attacks.

A node in Fig. 1(a) is removed by random failures or attacks and turns into the removed node in Fig. 1(b). Bypass rewiring is to directly connect each pair of links of the removed node like Fig. 1(c). Each pair of links for rewiring can be chosen by various ways including random selection like random bypass rewiring and heuristic methods like greedy bypass rewiring algorithm. If the degree of the removed node is odd, one link remains open. For example, an engineer or equipment can simply rewire cables (links) of a router (node) on the Internet (network) and relay (and sometimes amplify) the signals directly when the router does not work under random failures or attacks.

In this paper, we use generating functions based on the generating function formalism introduced in [4, 13, 14, 20]. We define

$$G_0(x) = \sum_{k=0}^{\infty} p_k x^k, \quad (1)$$

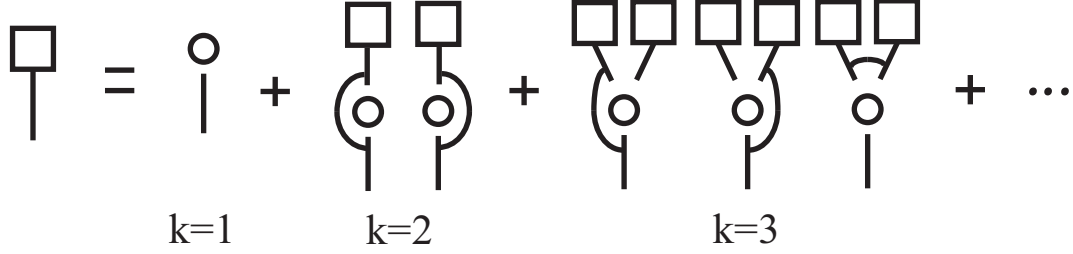


FIG. 2. Schematic diagram to calculate the probability that a component(square) is reached by a randomly chosen link with random bypass rewiring under removal of a node(circle).

$$G_1(x) = \frac{\sum_{k=1}^{\infty} k p_k x^{k-1}}{\sum_{k=1}^{\infty} k p_k} = \sum_{k=0}^{\infty} q_k x^k, \quad (2)$$

$$H_1(x) = \sum_{k=0}^{\infty} h_k x^k, \quad (3)$$

where p_k is the probability that a randomly chosen node has degree k and h_k is the probability that a randomly chosen link reaches a small component which has k nodes. In Eq. (2), q_k is the probability that a randomly chosen link reaches a node with degree k . Since nodes of the giant component do not belong to any small component which has fixed number of nodes on an infinite network, the probability that a randomly chosen node belongs to the giant component is

$$S = \sum_{k=0}^{\infty} p_k \phi_k \{1 - [H_1(1)]^k\} = \sum_{k=0}^{\infty} p_k \phi_k (1 - u^k), \quad (4)$$

for

$$H_1(x) = \sum_{k=0}^{\infty} q_k \{1 - \phi_{k+1} + \phi_{k+1} [H_1(x)]^k\}, \quad (5)$$

$$H_1(1) = u = f_1(u) = \sum_{k=0}^{\infty} q_k (1 - \phi_{k+1} + \phi_{k+1} u^k), \quad (6)$$

where ϕ_k is the occupation probability that a randomly chosen node with degree k is not removed and u is the smallest non-negative real solution of Eq. (6), that is, u is the average probability that a randomly chosen node is not connected to the giant component [3, 13, 14].

The average occupation probability is

$$\phi = \sum_{k=0}^{\infty} p_k \phi_k. \quad (7)$$

Based on the idea of Fig. 2, $H_1(x)$ and u satisfy

$$H_1(x) = q_0\phi_1x + q_0(1 - \phi_1) + q_1\phi_2xH_1(x) + q_1(1 - \phi_2)H_1(x) + q_2\phi_3x[H_1(x)]^2 + \frac{2}{3}q_2(1 - \phi_3)H_1(x) + \frac{1}{3}q_2(1 - \phi_3) + \dots \quad (8)$$

$$= \sum_{k=0}^{\infty} q_k\phi_{k+1}x[H_1(x)]^k + H_1(x) \sum_{k=0}^{\infty} q_k(1 - \phi_{k+1}) + [1 - H_1(x)] \sum_{\frac{k}{2}=0}^{\infty} \frac{p_{k+1}(1 - \phi_{k+1})}{\sum_{k=1}^{\infty} kp_k}, \quad (9)$$

$$u = f_2(u) = \sum_{k=0}^{\infty} q_k\phi_{k+1}u^k + u \sum_{k=0}^{\infty} q_k(1 - \phi_{k+1}) + (1 - u) \sum_{\frac{k}{2}=0}^{\infty} \frac{p_{k+1}(1 - \phi_{k+1})}{\sum_{k=1}^{\infty} kp_k}, \quad (10)$$

when random bypass rewiring is applied to an infinite network. In case of random failures ($\phi = \phi_k$), Eq. (10) corresponds to

$$u = f_3(u) = \phi \sum_{k=0}^{\infty} q_k u^k + (1 - \phi)u + (1 - u)(1 - \phi) \sum_{\frac{k}{2}=0}^{\infty} \frac{p_{k+1}}{\sum_{k=1}^{\infty} kp_k}. \quad (11)$$

The self-consistent equations like Eqs. (6) and (10) can be solved as follows by the fixed-point iteration which is a numerical method [21]. Iterating

$$u_{i+1} = f_1(u_i), \quad (12)$$

$$v_{i+1} = f_2(v_i), \quad (13)$$

for $u_0 = v_0 = 0$, u_i and v_i approaches to \bar{u} and \bar{v} , respectively, as i goes to infinity, for $\bar{u} = f_1(\bar{u})$ and $\bar{v} = f_2(\bar{v})$. Since the right hand side of Eq. (6) is equal to or larger than the right hand side of Eq. (10) for $0 \leq u \leq 1$, $u_i \geq v_i$ is satisfied for all i . Therefore, S with random bypass rewiring is always equal to or larger than without random bypass rewiring, that is, the percolation threshold with random bypass rewiring is always equal to or smaller than without random bypass rewiring.

To simulate attacks, a node with the highest degree is firstly removed and nodes are removed one by one in decreasing order of degree while randomly chosen nodes are removed one by one in case of random failures. In the simulation, degree of each node is not recalculated while nodes are removed. To simulate random bypass rewiring, each pair of links of the removed node are randomly chosen and rewired until no or one link remains.

For

$$p_{2k+1} = 0, \quad (14)$$

the smallest non-negative real solution of Eq. (10) is $u = 0$ since the last term of the right side of Eq. (10) is 0. The smallest non-negative real solution of Eq. (11) is also $u = 0$

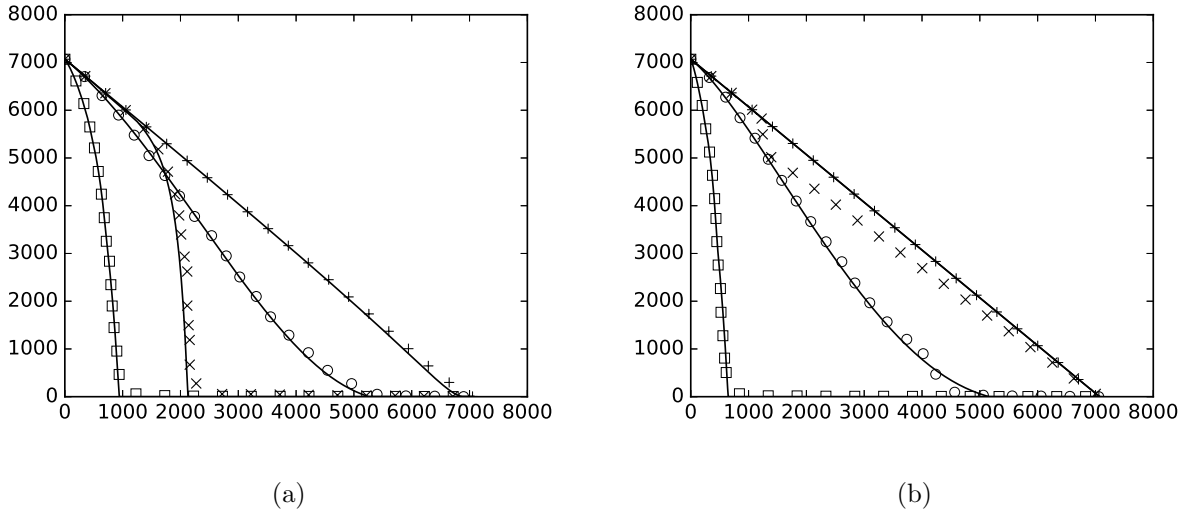


FIG. 3. The size of the largest component with respect to the number of removed nodes under random failures (circles/plus signs) and attacks (squares/crosses) without/with random bypass rewiring. The solid lines are for the numerically calculated S with respect to $N(1 - \phi)$ from Eqs. (4), (6), (10), and (11) on an infinite network with the same degree distributions. (a) On the undirected scale-free network generated by the degree distribution $p_k \sim k^3$ with $N = 7071$ nodes and $M = 10325$ links. (b) On the undirected even degree scale-free network generated by the degree distribution $p'_{2k} = p_{2k} + p_{2k+1}$ with $N = 7071$ nodes and $M = 9448$ links. Two straight lines for random bypass rewiring are overlapped.

for the same reason. Therefore, S is equal to ϕ and the percolation threshold is 0 on an even degree infinite network with random bypass rewiring for arbitrary ϕ_k . In other words, even degree networks randomly generated are extremely robust against removal of nodes including random failures and attacks with random bypass rewiring. Fig. 3(b) shows that almost all the nodes except the removed nodes on the even degree network are connected by random bypass rewiring. Every percolation threshold with random bypass rewiring in Fig. 3(b) is 0 while every percolation threshold in Fig. 3(a) is not.

The even degree network for Fig. 3(b) is generated by the degree distribution $p'_{2k} = p_{2k} + p_{2k+1}$ where p_k is the degree distribution of the original network for Fig. 3(a). For this reason, the original network has more links and larger average degree than the even degree network has. Without random bypass rewiring, the size of the largest component and S on the original network is larger than on the even degree network, respectively. On the other

hand, with random bypass rewiring, the size of the largest component and S on the even degree network are larger than on the original network, respectively, as seen in Fig. 3. In other words, the even degree network is more robust than the original network with random bypass rewiring while the original network is more robust than the even degree network without random bypass rewiring.

We propose a greedy bypass rewiring algorithm to improve robustness of networks against removal of nodes including random failures and attacks. The algorithm chooses a pair of link at each step, based on the number of the links not yet rewired and the size of the neighboring components.

A removed node with degree k has k neighbor nodes(neighbor 1, neighbor 2, \dots , neighbor k) and k links(link 1, link 2, \dots , link k). R_i denotes whether link i is rewired($R_i = 1$) or not yet rewired($R_i = 0$). Initially, set $R_i = 0$ for all i . $T_{i,j}$ denotes whether neighbor i and neighbor j belong to the same component($T_{i,j} = 1$) or do not($T_{i,j} = 0$), that is, there exists a path from neighbor i to neighbor j without going through the removed node or does not. Trivially, set $T_{i,i} = 1$ for all i . $\sum_{j=1}^k T_{i,j}(1 - R_j)$ denotes how many links in the component to which neighbor i belongs are not yet rewired. S_i denotes the size of the component to which neighbor i belongs. At t -th step for $1 \leq t \leq \lfloor \frac{k}{2} \rfloor$, choose α' which satisfies $R_{\alpha'} = 0$ and $\sum_{j=1}^k T_{\alpha',j}(1 - R_j) \geq \sum_{j=1}^k T_{i,j}(1 - R_j)$ for all i . From chosen α' , choose α which satisfies $R_\alpha = 0$, $\sum_{j=1}^k T_{\alpha,j}(1 - R_j) = \sum_{j=1}^k T_{\alpha',j}(1 - R_j)$, and $S_\alpha \geq S_i$ for all i . Update $R_\alpha = 1$. If $T_{i,j} = 1$ is satisfied for all i and j , choose randomly β which satisfies $R_\beta = 0$ without choice of β' . Otherwise, choose β' which satisfies $R_{\beta'} = 0$, $T_{\alpha,\beta'} = 0$, $\sum_{j=1}^k T_{\beta',j}(1 - R_j) \geq \sum_{j=1}^k T_{i,j}(1 - R_j)$ for all i . From chosen β' , choose β which satisfies $R_\beta = 0$, $T_{\alpha,\beta} = 0$, $\sum_{j=1}^k T_{\beta,j}(1 - R_j) = \sum_{j=1}^k T_{\beta',j}(1 - R_j)$, and $S_\beta \geq S_i$ for all i . Update $R_\beta = 1$. When neighbor α and neighbor β do not belong to the same component($T_{\alpha,\beta} = 0$), update the size of the component to which neighbor α and neighbor β belong($S_\alpha = S_\beta = S_\alpha + S_\beta$). Update $T_{\alpha,i} = T_{i,\alpha} = 1$ if there exists i which satisfies $T_{\beta,i} = T_{i,\beta} = 1$. Update $T_{\beta,i} = T_{i,\beta} = 1$ if there exists i which satisfies $T_{\alpha,i} = T_{i,\alpha} = 1$. Repeat each step of the algorithm $\lfloor \frac{k}{2} \rfloor$ times whenever a node is removed.

If there exists $i \neq \alpha, \beta$ which satisfies $\sum_{j=1}^k T_{i,j}(1 - R_j) > 1$, the maximum size of the largest component is not guaranteed for $\sum_{j=1}^k T_{\alpha,j}(1 - R_j) \leq 1$ or $\sum_{j=1}^k T_{\beta,j}(1 - R_j) \leq 1$. From this aspect, we choose α' and $\beta' \neq \alpha$ which maximize $\sum_{j=1}^k T_{\alpha',j}(1 - R_j)$ and $\sum_{j=1}^k T_{\beta',j}(1 - R_j)$ in the algorithm. If $\sum_{j=1}^k T_{i,j}(1 - R_j) \leq 1$ is satisfied for all $i \neq \alpha$, the

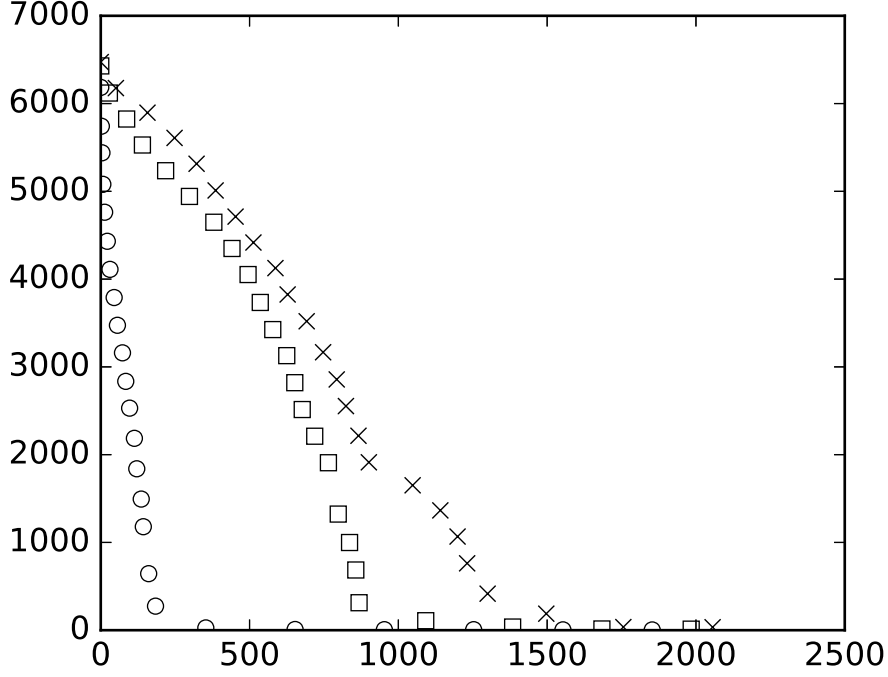


FIG. 4. The size of the largest component with respect to the number of removed nodes on the autonomous system(AS-733) from [22] with $N = 6474$ nodes and $M = 12572$ links under attacks. The circles are for the case without bypass rewiring. The squares/crosses are for the case with random bypass rewiring/greedy bypass rewiring.

maximum size of the largest component is not guaranteed when there exists i which satisfies $S_\beta < S_i$. If $\sum_{j=1}^k T_{i,j}(1 - R_j) \leq 1$ is satisfied for all i , the maximum size of the largest component is not guaranteed when there exists i which satisfies $S_\alpha < S_i$ or $S_\beta < S_i$. From this point of view, we choose α and $\beta \neq \alpha$ which maximize S_α and S_β in the algorithm for $\sum_{j=1}^k T_{\alpha,j}(1 - R_j) = \sum_{j=1}^k T_{\alpha',j}(1 - R_j)$ and $\sum_{j=1}^k T_{\beta,j}(1 - R_j) = \sum_{j=1}^k T_{\beta',j}(1 - R_j)$. Therefore, the algorithm guarantees the maximum size of the largest component at each step where which node will be removed next is unknown.

Fig. 4 shows that the greedy bypass rewiring algorithm improves the robustness of the Internet under attacks more than random bypass rewiring. Since we ignore and eliminate self links and double links for the simulation, the number of links on the network is 12572 where the network originally has 13895 links.

In summary, we have introduced a concept of bypass rewiring and analytically and numer-

ically investigated random bypass rewiring with simulations. The results have shown that random bypass rewiring improves robustness of networks under removal of nodes including random failures and attacks. With random bypass rewiring, all nodes except the removed nodes on an even degree infinite network are connected for arbitrary occupation probabilities and then the percolation threshold is 0. With/without random bypass rewiring, the size of the largest component and S on the original network are smaller/larger than on the even degree network randomly generated by the degree distribution $p'_{2k} = p_{2k} + p_{2k+1}$, respectively, where p_k is the degree distribution of the original network. It means that random bypass rewiring makes even degree networks extremely robust. Based on the number of the links not yet rewired and the size of the neighboring components, we have proposed a greedy bypass rewiring algorithm which guarantees the maximum size of the largest component at each step, assuming that which node will be removed next is unknown. The simulation result has shown that the algorithm improves robustness of the autonomous system of the Internet more than random bypass rewiring. We hope that bypass rewiring equipment is implemented and added on the existing routers on the Internet. More various applications and studies of bypass rewiring in many fields are expected.

-
- [1] R. Albert, H. Jeong, and A.-L. Barabasi, *Nature (London)* **406**, 378 (2000).
 - [2] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, *Phys. Rev. Lett.* **85**, 4626 (2000).
 - [3] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, *Phys. Rev. Lett.* **86**, 3682 (2001).
 - [4] M. E. J. Newman, S. H. Strogatz, and D. J. Watts, *Phys. Rev. E* **64**, 026118 (2001).
 - [5] S. N. Dorogovtsev and J. F. F. Mendes, *Adv. Phys.* **51**, 1079 (2002).
 - [6] V. Latora and M. Marchiori, *Physica A* **314**, 109 (2002).
 - [7] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, *Phys. Rev. E* **65**, 056109 (2002).
 - [8] R. Albert and A.-L. Barabasi, *Rev. Mod. Phys.* **74**, 47 (2002).
 - [9] M. E. J. Newman, *SIAM Rev.* **45**, 167 (2003).
 - [10] S. Boccaletti, V. Latora, M. Marchiori, and A. Rapisarda, *Phys. Rep.* **424**, 175 (2006).
 - [11] P. Crucitti, V. Latora, and S. Porta, *Phys. Rev. E* **73**, 036125 (2006).
 - [12] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, *Proc. Natl. Acad. Sci. USA* **108**, 3838 (2011).

- [13] M. E. J. Newman, *Networks: An Introduction* (Oxford University Press, Oxford, 2010).
- [14] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).
- [15] L. K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, Phys. Rev. Lett. **94**, 188701 (2005).
- [16] S. N. Dorogovtsev and A. V. Goltsev, Rev. Mod. Phys. **80**, 1275 (2008).
- [17] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, Physica A **357**, 593 (2005).
- [18] S. Xiao, G. Xiao, T. H. Cheng, S. Ma, X. Fu, and H. Soh, Europhys. Lett. **89**, 38002 (2010).
- [19] W. Quattrociocchi, G. Caldarelli, and A. Scala, PLoS ONE **9**, e87986 (2014).
- [20] H. S. Wilf, *Generatingfunctionology*, 2nd ed. (Academic Press, London, 1994).
- [21] R. L. Burden and J. D. Faires, *Numerical Analysis*, 9th ed. (Brooks/Cole, Boston, MA, 2011).
- [22] J. Leskovec and A. Krevl, “SNAP Datasets: Stanford large network dataset collection,” <http://snap.stanford.edu/data> (2014).